Banking Fraud Control Comparison Data

The main current account providers have agreed to publish information about their approach to fraud prevention. The information included below is provided on a voluntary basis and comparative data can be found on the FCA's website

Fraud Prevention Philosophy	
What is your approach to Fraud Prevention?	Bank of Scotland adopts an approach to fraud risk management that seeks to balance the demands of driving down fraud losses, whilst being sensitive to the impact(s) on customer experience and operational demands. We do this by using the latest tools and industry best practice to create an environment that is unattractive to fraudsters and that protects and serves our customers, regardless of their product or channel of choice.
What controls do you have in place / How do we protect you?	We protect your money by using real time fraud detection systems to monitor transactions on your accounts. We utilise various tools such as device identification of the phones, tablets etc. that you use, in conjunction with biometric behavioural analysis to identify potential fraudulent activity. Furthermore, we adopt a multi-channel approach to authentication. When you call our Telephone Centre, log into Internet Banking or pop into branch we will carry out verification checks to make sure it is you we are talking to. In addition to using your memorable information, personal security number or password information, we also use biometric technology to identify you, for example voice ID on our telephony channel, which allows you to use your voice as your password. When logging on to the mobile banking App, customers are able to use their Touch ID to authenticate themselves instead of their password. For some online card transactions and wallet pay card registrations, we will double check that it is you making the payment or completing the registration by sending a 'one time passcode' to your phone, which you can enter into the screen to complete the transaction. In the event that suspicious activity is identified we will attempt to contact you to verify. We work with the card issuer under their chargeback scheme, which means that we can often recover your money directly from them for fraud transactions. In addition, we have developed and fully apply best practice standards with the industry and regulators to ensure that authorised push payment fraud cases are dealt with efficiently, consistently and fairly by both the sending and receiving bank. Where funds have fraudulently been taken from your account, we will work with the bank that received the funds, under an indemnity scheme to recover any remaining funds.

Customer Education & Awareness	
What do you do to educate your customers to ensure they are fully aware of the latest fraud trends / advice?	Education and Awareness is undertaken across a number of mediums for both our customers and colleagues. Relating this to the latest fraud Modus Operandi [MO] is seen as vitally important by Bank of Scotland, to help protect customers from falling victim to fraud. Bank of Scotland is also a signatory to the Take Five Charter and adheres to the minimum standards. All customer facing colleagues complete annual mandatory training which covers scams and how to spot them, as well as a refresher for the Banking Protocol process to help them best support customers. Furthermore regular communications are issued to front line colleagues as new trends emerge. Our online branded .com websites, have specific fraud/scam awareness pages which are regularly updated and have educational information on various different types of frauds, how to protect yourself and what to do if you become a victim. We also email customers messages relating to fraud prevention and regularly post this information on our social media channels. When a customer is transacting on their online banking, we also provide targeted, in-session, tailored messaging warning customers about common fraud MO's. Our branch network has an array of collateral available including posters, videos and leaflets. Fraud surgery's, fronted by the Dedicated Card and Payment Crime Unit (DCPCU) are also held in branches and Bank buildings to educate customers and colleagues about the different types of fraud. Our ATMs and IDMs (Immediate Deposit Machines) contain fraud prevention messages.
Contact	
How and when we would contact our customers.	We will contact you using phone calls, text messages and onscreen notifications. Customers are encouraged to always take the necessary precaution to ensure they are talking to who they think they are. We also utilise various security prevention and detection controls, which can trigger manual and automatic customer contact, examples include: • **One-time passcodes -** When we need to verify who you are, we'll send a unique code to the mobile we have registered for you. The text will state exactly what the code is for, and you shouldn't tell anyone what this code is other than the bank.

	• **New Beneficiary Recipient –** When you set up a new beneficiary we will send confirmation to the mobile number we have registered for you. The text will state the date and time this was added to your account, and what to do if this wasn't you. While we may ask you to reply to messages, we'll never: • Include a link to the log in pages of our own websites. • Ask for your complete security number, password, or card number. • Ask you for answers to your security questions. We offer guidance for identifying both scam calls and messages on our website, however if you're not sure whether a call, text or email is genuine, you can contact us on the following number: • 03457 213141

How and when can our customers contact us?	• In the UK: If you are a victim or fraud, or require any fraud prevention advice we offer a 24/7 service to all our customers, who can contact us on:
	
	  • 03457 213141
	
	• Outside of the UK:
	
	  • +44(0)131 337 4218
	
	• Customers requiring additional support: If you have a hearing or speech impairment, you can contact us 24/7 using the Next Generation Text (BGT) Service. If you're Deaf and a BSL user, you can use the SignVideo service.

How we collaborate with the rest of the industry	
Industry initiatives / collaboration	• We are members of UK Finance and take an active part in all Industry fraud & financial crime initiatives. • We are active members of CIFAS. • We contribute to the funding of the Dedicated Card and Payment Crime Unit (DCPCU) who work to identify and target the organised criminal gangs. • We share fraud intelligence to protect our customers, working with the National Crime Agency and other law enforcement and intelligence agencies. • We have signed up to the Take Five Charter to provide our customers with up to date advice.

	• We champion and participate in the Banking Protocol. • We collaborate with other banks to quickly recover fraudulent funds for our customers and have signed up to Contingent Reimbursement Model (CRM), which sets out the circumstances when payment service providers are responsible for reimbursing APP scam victims. • We are signed up to implement confirmation of payee. • We have partnered with City of London Police, investing £1.5 million in the force's Economic Crime Directorate. • We have partnered with Trading Standards to support their Friends Against Scams campaign. • We work in collaboration with the Regulator and ICO to ensure a collective response to fraud & financial crime.
Summary	
Summary	Helping keep our customers' money safe is a top priority and we have sophisticated, multi-layered defences to help protect our customers from criminals. We are continually strengthening our defences using new technology, analysing data in real-time to stop fraud happening in the first place. If we do spot suspicious activity on a customer's account, we will contact them immediately. In addition, we have dedicated resources online, printed material available in our branches and all our colleagues in branch and over the phone are trained to be able to assist our customers with any fraud prevention related questions.